J. Soc. Korea Ind. Syst. Eng Vol. 41, No. 4 : 179-188, December 2018
https://doi.org/10.11627/jkise.2018.41.4.179
ISSN : 2005-0461(print)
ISSN : 2287-7975(online)

Performance Improvement of Distributed Consensus Algorithms for Blockchain through Suggestion and Analysis of Assessment Items

Do Gyun Kim* · Jin Young Choi*† · Kiyoung Kim** · Jintae Oh**

*Department of Industrial Engineering, Ajou University
**Electronics and Telecommunications Research Institute

평가항목 제안 및 분석을 통한 블록체인 분산합의 알고리즘 성능 개선

김도균* · 최진영*† · 김기영** · 오진태**

*아주대학교 산업공학과
**한국전자통신연구원

Recently, blockchain technology has been recognized as one of the most important issues for the 4th Industrial Revolution which can be represented by Artificial Intelligence and Internet of Things. Cryptocurrency, named Bitcoin, was the first successful implementation of blockchain, and it triggered the emergence of various cryptocurrencies. In addition, blockchain technology has been applied to various applications such as finance, healthcare, manufacturing, logistics as well as public services. Distributed consensus algorithm is an essential component in blockchain, and it enables all nodes belonging to blockchain network to make an agreement, which means all nodes have the same information. For example, Bitcoin uses a consensus algorithm called Proof-of-Work (PoW) that gives possession of block generation based on the computational volume committed by nodes. However, energy consumption for block generation in PoW has drastically increased due to the growth of computational performance to prove the possession of block. Although many other distributed consensus algorithms including Proof-of-Stake are suggested, they have their own advantages and limitations, and new research works should be proposed to overcome these limitations. For doing this, above all things, we need to establish an evaluation method existing distributed consensus algorithms. Based on this motivation, in this work, we suggest and analyze assessment items by classifying them as efficiency and safety perspectives for investigating existing distributed consensus algorithms. Furthermore, we suggest new assessment criteria and their implementation methods, which can be used for a baseline for improving performance of existing distributed consensus algorithms and designing new consensus algorithm in future.

Keywords : Blockchain, Distributed Consensus Algorithm, Performance Assessment, Safety Assessment

Received 12 November 2018; Finally Revised 12 December 2018;
Accepted 13 December 2018
† Corresponding Author : choijy@ajou.ac.kr

1. 서 론

블록체인(Blockchain) 기술은 필요한 데이터를 블록 형태로 저장하고, 이러한 블록들을 암호화 기술 기반으로 연결된 하나의 체인으로 관리하기 위한 기술이다[15]. 이 때, 각각의 블록은 이전 블록의 해시 값과 시간 정보, 트랜잭션 데이터 등을 포함하며, 체인에 등록된 블록은 검증 가능하며 비가역적인(irreversible) 방법으로 기록되어 내용을 수정하기 어려운 구조로 되어 있다. 블록체인에 참여하는 노드들이 분산된 환경에서 별도의 중앙 기관이나 관리자 없이 P2P(Peer-to-Peer) 네트워크를 통해 연결되어 있으면서 체인에 기록된 정보를 포함하고 있기 때문에 블록체인은 일종의 분산된 원장(distributed ledger)이라고 할 수 있다.

이와 같이 비가역적인 체인의 형태로 데이터를 저장하는 시도는 이전에도 존재하였으나[10], 현재와 같은 블록체인 기술을 성공적으로 구현한 최초의 사례는 Satoshi [14]라고 할 수 있다. 해당 논문에서는 복잡한 연산을 수행하고, 수행된 연산을 증명하여 블록을 생성하는 P2P 네트워크 기반의 암호화폐인 비트코인을 제안하였다. 비트코인의 가장 큰 특징은 연산량에 대한 증명을 토대로 보상을 주는 시스템을 구현하였다는 점이다. 이를 통해, 사용자는 자신이 가진 컴퓨팅 성능을 악의적인 공격을 위해 사용하는 것보다 정직하게 계산을 위해 사용할 때 더 많은 편익을 얻을 수 있다. 또한, 사용자와 사용자의 상호작용 관점에서는 P2P 네트워크를 통해 중개 기관 없는 거래 수행을 지원한다. 이러한 특징은 기존 금융 시스템과 다르게 사용자들이 직접 거래를 수행할 수 있으면서도 익명성과 보안성이 유지되는 전자 금융 시스템을 구축할 수 있도록 할 수 있다.

세계경제포럼(World Economy Forum)의 2016년 보고서에서는 사회 변혁을 위한 21가지 기술 중 하나로 블록체인을 지목하였으며[21], 전반적으로 블록체인은 인공지능과 사물 인터넷 결합으로 대두될 4차 산업 혁명을 이끌어갈 수 있는 핵심 기술로 평가되고 있다. 현재 블록체인 기술은 다양한 응용 분야에 적용되고 있으며, 암호화폐를 포함한 금융 분야는 블록체인이 가장 두각을 드러내는 분야이다. 금융 분야의 블록체인은 결제 시스템의 절차를 간소화하거나 중개기관의 필요성을 배제하고 거래 시간을 단축할 수 있는 금융 시스템의 구현, 거래 내역의 검증을 통한 보안 성능 개선 등으로 적용 범위를 넓혀가고 있다[18]. 환자의 상태와 건강 검진 결과 등의 의료 정보를 기록하고 공유할 수 있는 헬스케어 시스템 또한 블록체인 기술을 통해 구현될 수 있는 분야이다[1]. 제조와 물류 분야에서는 분산 원장 기술이라는 특성을 이용하여 제품의 생산 과정에서 발생할 수 있는 데이터를 관리하거나, 공급망에 블록체인 개념을 적용하여 물류 프로세스를 개선하는 시도가 이루어지고 있다[12, 20]. 그 외에도, 개인의 신원 정보를 저장하고 이를 통해 신원을 확인하거나 공문서 등의 기록물을 관리하는 기능을 통해 공공 서비스 분야에도 블록체인이 적용되고 있다[17].

이러한 응용에서 블록체인은 분산된 환경에서 각각의 노드들이 블록을 생성하고 자신이 생성한 블록의 정보를 전파하거나, 다른 노드가 생성한 블록에 대한 정합성 판별 및 검증을 수행할 수 있도록 한다. 이 과정에서, 각각의 노드들 사이에 이루어진 트랜잭션에 대한 기록이나 블록 생성 및 검증을 위한 내용들은 모든 노드에서 동일하게 기록되어야 한다. 이 때, 블록체인에 참여하는 모든 노드가 동일한 정보를 기록하고 있는 상태를 유지하기 위해 사용되는 프로토콜이 분산합의 알고리즘이다[2]. 즉, 분산합의 알고리즘이란 분산된 환경에서 복수의 주체가 협업하는 과정 중에 발생할 수 있는 불일치를 해결하여 시스템을 통일된 상태로 유지하기 위한 알고리즘으로써 블록체인에서 가장 중요한 역할을 수행한다.

가장 대표적인 암호화폐인 비트코인이나 이더리움은 고도의 연산량을 바탕으로 블록의 생성과 검증을 수행하고, 확정된 블록에 대한 정보를 모든 주체에게 전파하는 분산합의 알고리즘을 사용한다. 그러나 이러한 방식은 블록 생성을 위해 필요한 연산량이 점차 증가하여 에너지와 컴퓨팅 자원의 지나친 낭비를 가져오기 때문에 이에 대한 새로운 대안이 요구되어져 왔다[4]. 이후에 다양한 분산합의 알고리즘이 제안되었지만, 각각 본연의 한계점들을 가지고 있어 새로운 합의 알고리즘에 대한 연구가 지속적으로 필요하다.

그러나 이를 위해서는 먼저 지금까지 제안된 분산합의 알고리즘을 평가하기 위한 항목을 도출하고, 이에 기반하여 기존 알고리즘들의 장단점을 면밀히 검토하는 것이 필요하다. 이러한 목적으로 본 논문에서는 기존 분산합의 알고리즘들의 성능 평가항목을 효율성 지표와 안전성 지표로 구분하여 제시하고, 이를 기준으로 기존 알고리즘들을 분석한 결과를 제시하였다. 또한 기존 알고리즘들에 고려되지 않은 새로운 지표와 이에 대한 구현 방안을 제시함으로써 향후 새로운 분산합의 알고리즘의 설계에 고려될 수 있도록 하였다.

본 논문의 구성은 다음과 같다. 먼저, 제 2장에서는 현재까지 제안된 기존 분산합의 알고리즘에 대해 기술한다. 제 3장에서는 조사된 분산합의 알고리즘을 평가하기 위한 핵심 지표들을 선정하고, 각 지표에 대한 분석을 수행한다. 제 4장에서는 기존 분산합의 알고리즘을 개선하기 위한 방안을 탐색하며, 제 5장에서 논문의 결론을 기술한다.

2. 블록체인 분산합의 알고리즘

블록체인은 P2P 네트워크에 참여하는 노드들의 권한에 따라 퍼블릭, 프라이빗, 그리고 두 가지 특징을 모두 포함하고 있는 하이브리드 블록체인으로 나눌 수 있으며, 각각의 특징은 다음과 같다.

2.1 퍼블릭 블록체인의 분산합의 알고리즘

2.1.1 작업 증명(Proof-of-Work, PoW)[14]

작업 증명 알고리즘을 이용하는 블록체인 시스템에서는 모든 노드가 블록 생성 권한을 가지고 있으며, 블록 생성은 전체 노드의 경쟁을 통해 이루어진다. 이때, 각 노드는 고도의 컴퓨팅 능력을 요구하는 해시 퍼즐의 답을 찾기 위한 작업을 수행하게 되며, 해시 퍼즐의 답을 가장 빠르게 찾은 노드가 블록 생성에 성공하게 된다. 해시 퍼즐 문제는 식 (1)과 같은 난이도 조건을 충족하는 입력 값을 찾는 것을 목표로 하며, 입력 값인 난스(nonce)를 생성된 블록의 헤더 부분에 기록한다[4].

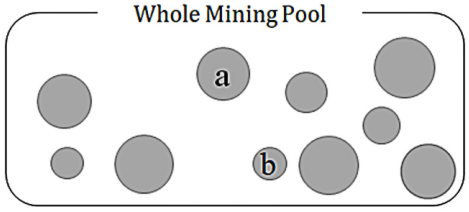
$$hash(B) \leq M/D \tag{1}$$

여기서 M은 이론적으로 가능한 최대 난이도 값이며, D는 현재 사용되는 난이도 값을 의미한다. 작업 증명 알고리즘을 이용하는 블록체인에서는 D의 값을 조절하여 난스 값을 찾는 것을 어렵게 만들 수 있으며, 이를 통해 블록 생성의 속도를 유지하고 생성된 블록의 가치를 유지할 수 있다.

그러나 더 많은 블록이 생성됨에 따라 난이도가 상승하여 해시 퍼즐의 답을 찾기 위한 과정에서 요구되는 연산량이 증가하고, 블록 생성에 사용되는 에너지 소모량이 매우 커질 수 있다. 작업 증명 알고리즘은 최초의 암호화폐인 비트코인에서 사용되었으며, 이후에 등장한 이더리움, 라이트코인 등의 다른 암호화폐 역시 마찬가지로 작업 증명 알고리즘을 통해 운영되고 있다.

2.1.2 지분 증명(Proof-of-Stake, PoS)[6, 11]

지분 증명 방식 합의 알고리즘은 작업 증명 알고리즘의 단점인 블록 생성에 사용되는 에너지 소모량을 극복하기 위한 대안으로 제시되었다. 작업 증명의 경우와 마찬가지로 모든 노드가 블록 생성을 위한 권한을 가지고 있으며, 각 노드는 보유한 지분(stake)에 비례하는 확률에 따라 블록 생성에 성공하게 된다. 예를 들어, 지분 증명 알고리즘을 통해 블록을 생성하고자 하는 노드들과 그 지분의 크기가 <Figure 1>과 같다면, 지분의 크기가 큰 노드 a가 b보다 높은 확률로 블록을 생성할 수 있다.



Size of stakes that belonging to nodes : a > b

→ Probability of block generation : a > b

<Figure 1> Effect of Stake in Proof-of-Stake Consensus

그 외에도, 지분 증명 알고리즘은 작업 증명 알고리즘과 혼합하여 사용하는 것이 가능하다. 구체적으로는 식 (2)와 같이 작업 증명 알고리즘에서 사용되는 해시 퍼즐의 난이도를 지분에 따라 달라지도록 수정하여 더 많은 지분을 가진 노드가 더 높은 확률로 블록을 생성할 수 있도록 할 수 있다[4].

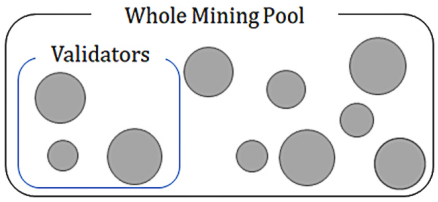
$$hash(hash(B_{prev}), A, t) \leq bal(A) \times M/D \tag{2}$$

여기서 B_{prev}는 해당 블록 생성의 기준이 되는 이전 블록을 지칭하며, $A, bal(A), t$는 각각 블록을 생성하고자 하는 노드, 해당 노드가 가진 지분의 잔액, 블록을 생성하는 시점을 나타낸다.

지분 증명 알고리즘은 합의 과정에서 지분을 가진 모든 노드가 참여하는 방식으로 인해 각각의 노드가 가진 지분에 대한 검증이 요구되며, 이는 합의 과정에서의 비효율성을 야기할 수 있다는 단점이 있다. 또한, 보유한 지분이 새로운 블록의 소유권을 높은 확률로 보장해주기 때문에, 지분의 독과점이 일어날 수 있다. 지분 증명 알고리즘을 이용하는 블록체인으로는 작업 증명 알고리즘에 지분 증명을 적용하여 에너지 소모량을 줄인 피어코인, 작업 증명을 배제하고 순수 지분 증명을 통해 블록 생성을 수행하는 암호화폐 Nxt 등이 있다.

2.1.3 위임된 지분 증명(Delegated Proof-of-Stake, DPoS)[4]

지분 증명 방식의 합의 알고리즘이 합의에 도달하기 어렵게 만드는 형태의 공격을 허용할 수 있음을 보완하기 위해, <Figure 2>와 같이 권한을 위임받은 대표자들을 선정하여 블록 생성과 검증에 대한 권한을 부여하는 위임된 지분 증명 방식이 제안되었다. 이때, 대표자 선출은 투표를 통해 이루어지며, 모든 노드는 자신이 가진 지분에 비례한 투표권을 행사할 수 있다. 선정된 대표자들에 의한 블록 생성 및 검증 과정을 통해 기존 지분 증명 알고리즘보다 합의를 위한 시간과 비용 절약이 가능하며, 블록 생성 효율성을 제고할 수 있다.



<Figure 2> Mining Pool of Delegated Proof-of-Stake

그러나 이러한 방법은 행사할 수 있는 투표권의 크기가 지분의 크기와 비례하기 때문에, 이로 인해 특정 주체들이 대표자의 위치를 독과점할 수 있다는 위험성이 있다. 또한, 블록 생성에 참여하는 주체가 대표자들로 한정되기 때문에, 네트워크를 통한 공격이 더욱 용이하게 이루어져 보안 성능에 취약점을 보일 수 있다. 블록체인을 이용하여 가상 자산의 중개 서비스를 제공하는 Bitshares, 암호화폐인 EOS, Ark 등에서 위임된 지분 증명 알고리즘이 합의를 위해 사용되고 있다. 그 외에 이더리움 또한 위임된 지분 증명 알고리즘으로 분산합의 알고리즘을 변경하려는 계획을 가지고 있다.

2.1.4 중요도 증명(Proof-of-Importance, PoI)[16]

중요도 증명 알고리즘은 지분 증명 알고리즘에서 지분이 특정 노드에 집중되는 문제점을 해결하기 위해 제안되었으며, 체인의 유동성과 거래 과정에 대해 노드가 기여한 바에 따라 측정되는 중요도에 따라 블록 생성의 권한을 부여한다. 작업 증명에서 사용되는 해시 퍼즐과 비슷하게, 식 (3)과 같은 중요도 기반의 해시 함수를 이용하여 블록을 생성한다.

$$2^{54}\left|\ln\left(\frac{h}{2^{256}}\right)\right| < 264\frac{b}{d}t \tag{3}$$

이때, h는 이전 블록의 해시와 노드의 공개키를 통해 만들어진 해시 값, d는 새로운 블록 생성의 난이도, t는 최근 블록 생성 후 지나간 시간, b는 해당 노드의 중요도를 의미한다. 즉, 노드의 중요도가 높을수록 블록을 생성할 확률이 높다. 중요도 증명 알고리즘은 암호화폐인 NEM에서 처음으로 이용되었다.

2.2 프라이빗 블록체인의 분산합의 알고리즘

2.2.1 소요 시간 증명(Proof-of-Elapsed Time, PoET)[9]

소요 시간 증명 알고리즘은 신뢰할 수 있는 실행 환경에서 합의가 수행된다. 블록 생성에 참여하는 노드들은 임의의 시간만큼 수행되는 대기 프로세스를 수행하고, 대기가 끝난 후 가장 짧은 시간 내에 응답한 노드가 블록을 생성하게 된다. 생성된 블록에 대한 검증은 프로토콜에서 정해진 대기 시간의 사용 횟수를 준수하여 블록을 생성하였는지 검토하여 이루어진다. 또한, 이러한 프로토콜을 숙지한 공격자가 응답 시간을 변경하며 블록을 과도하게 생성하였는지 검증하기 위해 한 노드가 특정 시간 동안 생성할 수 있는 블록 수를 정의하고, 이를 이용한 통계적 검증을 함께 수행한다. 이러한 과정은 컴퓨팅 자원이나 지분에 대한 독점과 중앙화 문제를 극복하고, 프로토콜을 통한 안전성과 임의 선택을 통한 공정성을 제고할 수 있는 토대가 된다. 그러나 전반적인 프로세스 및 프로토콜이 인텔의 SGX에 의해 이루어지기 때문에 이에 대한 의존성이 생기고 확장이나 응용에 대한 제약이 발생할 수 있다. Hyperledger의 Sawtooth가 소요 시간 증명 알고리즘을 채택하고 있다.

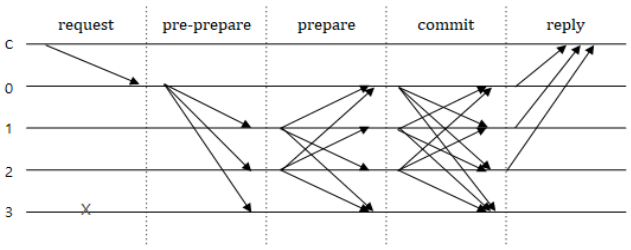
2.2.2 Paxos/Raft 알고리즘[8, 19]

블록체인 등장 이전부터 분산 시스템에서 사용되었던 Paxos/Raft 합의 알고리즘은 네트워크에 참여한 다수의 노드들로부터 여러 값들을 제안 받고 그 값들 중 하나를 선택하여 합의를 도출한다. 이 과정은 값을 제안하는 제안자와 제안된 값에 대해 판단을 내리는 수용자에 의해 이루어진다. 이 과정에서, 과반 수 이상의 동의를 얻은 제안이 합의 내용으로 기록된다. JP 모건의 퍼블릭 블록체인 프로젝트인 Quorum은 Raft 알고리즘을 분산합의 알고리즘으로 채택하고 있다.

2.2.3 Practical Byzantine Fault Tolerance(PBFT) 알고리즘[7]

Paxos/Raft 알고리즘이 비잔틴 노드에 대한 보호가 불가능한 점을 보완하기 위해 설계된 PBFT 알고리즘은 악의적인 노드의 존재에도 불구하고 합의를 도출할 수 있다. PBFT 알고리즘을 이용하는 블록체인에서는 의사 결정자의 역할을 수행하는 리더 노드가 존재하며, 구체적인 합의 과정은 <Figure 3>과 같이 이루어진다. 이때, 노드 C는 블록의 생성 및 검증에 대한 요청을 보내는 고객을 의미하며, 노드 0이 리더 노드, 노드 3은 악의적인 노드이다. 먼저, 블록 생성과 검증에 대한 요청을 받은 리더 노드는 사전 준비(pre-prepare) 단계에서 나머지 노드에게 메시지를 전송한다. 리더 노드의 메시지를 받은 다른 노드는 자신의 메시지를 검증하여 참이면 다른 모든 노드들에게 준비(prepare) 메시지를 보낸다. 각 노드들이 다른 노드로부터 받은 준비 메시지의 수가 전체 노드 수의 2/3이상이면 준비 단계에서의 합의가 이루어진 것으로 판단한다. 이후, 노드들은 블록에 대한 심사 여부를 검증하고 이에 대한 결정(commit) 메시지를 전송한다. 만일, 결정 메시지의 수가 2/3 이상이라면, 최종적으로 블록이 체인에 등록되는 것이 결정된다. 즉, PBFT 합의 알고리즘은 준비 단계에서 메시지에 대한 합의를, 결정

단계에서 블록에 대한 합의를 수행하여 총 2번의 합의 과정이 발생하게 된다. 이 과정에서 비잔틴 노드인 노드 3의 존재에도 불구하고, 2/3 이상의 동의가 이루어짐으로써 합의에 도달하는 것이 가능하다.

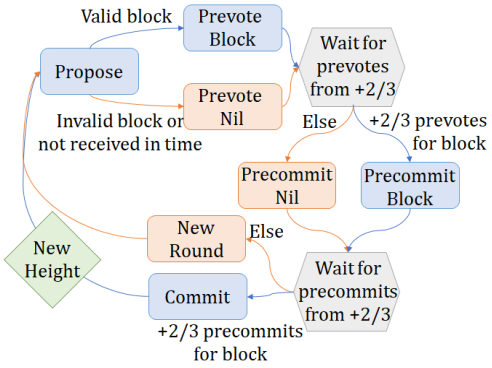


<Figure 3> Consensus Protocol of PBFT

또한, 리더 노드로부터 결정이 전파되어 나가는 과정을 통해 시스템 전체 흐름과는 다른 메시지를 보내어 체인이 분화되는 포크를 방지하고 고발할 수 있다는 특징을 가진다. 그러나 리더 노드와 나머지 노드의 역할이 미리 정의되어 있어야 신뢰성을 보장할 수 있기 때문에, 퍼블릭 블록체인에는 적용되기 어려운 특징을 가지고 있다. 블록체인 개발 솔루션 Monax와 암호화폐 리플 등이 PBFT 알고리즘을 이용하는 대표적인 블록체인이다.

2.3 하이브리드 분산합의 알고리즘

Tendermint[5]는 블록체인 개발을 위한 플랫폼인 코스모스에서 이용하고 있는 합의 알고리즘으로서, 기존의 PBFT 알고리즘이 퍼블릭 블록체인에서 사용되기 어려운 점을 극복하고자 도입되었다. 즉, 퍼블릭과 프라이빗 블록체인 모두에 적용 가능한 합의 알고리즘이라고 할 수 있다. Tendermint 합의 알고리즘에서는 공개키를 통해 식별된 검증인들들이 블록의 생성과 검증에 대한 의사결정을 수행하며, 검증인들은 지분에 따라 차등적인 투표권을 가진다. 즉, PBFT 알고리즘과 위임된 지분 증명 개념을 함께 적용하여 합의를 수행하는 알고리즘이라고 할 수 있다. 기본적인 합의 구조는 PBFT와 유사하지만, 전체 노드가 아닌 검증인 노드만이 투표에 참여한다는 것과 각 노드가 행사할 수 있는 투표권이 동일하지 않고 지분에 비례한다는 차이점이 있다. <Figure 4>는 Tendermint 합의 알고리즘의 구체적인 과정을 나타낸다. 블록이 제안되면(propose) 각각의 노드는 블록의 유효성에 대해 판단하고, 자신의 지분에 비례하여 주어지는 투표권을 행사한다(prevote). 블록이 전체 투표권 중 2/3 이상의 동의를 얻었다면, 블록이 유효한 블록으로 인정이 된다. 2/3의 동의가 전체 검증자들에게로 전파되고(precommit), 최종적으로 블록이 확정되어(commit) 블록체인 상의 새로운 높이(height)에 블록이 등록된다. 투표권의 2/3 이상이 동의하지 않은 경우에는 새로운 라운드(round)를 시작하여 다른 블록에 대한 제안이 가능하도록 한다.



<Figure 4> Consensus Protocol of Tendermint

3. 평가항목 제안 및 분석

지금까지 이러한 분산합의 알고리즘의 성능을 평가하여 체계적으로 분석한 연구는 없었다. 따라서 본 장에서는 이러한 분산합의 알고리즘에 대한 성능 평가항목을 효율성과 안전성으로 나누어 제시하고, 각 항목에 대해 다양한 분산합의 알고리즘을 비교·분석하고자 한다.

3.1 분산합의 알고리즘 평가항목 제안

3.1.1 효율성 평가항목

(1) 합의 노드의 수

합의 노드의 수는 블록체인 분산합의 알고리즘에서 합의 과정에 참여하는 노드의 수를 의미한다. 이는 최종적으로 합의에 도달하는 속도에 영향을 미치며, 합의 과정에서 교환되는 메시지의 규모, 즉 네트워크 통신량과 연관성을 가진다.

(2) 에너지 소모량

에너지 소모량은 블록을 생성하는 과정에서 발생하는 에너지 소모량을 나타낸다. 대표적인 암호화폐인 비트코인의 연간 에너지 소모량은 시간당 약 73.12 테라와트로 추정되며[3], 이와 같은 높은 에너지 소모량은 지분 증명 알고리즘과 같은 새로운 분산합의 알고리즘이 제안되도록 하였다.

(3) 초당 트랜잭션 처리량(Transaction Per Second, TPS)

초당 트랜잭션 처리량은 블록체인에 참여하는 주체들 사이에 발생하는 트랜잭션을 처리하고 기록하는 능력으로써 초당 처리량으로 표현하며, 분산처리 알고리즘의 핵심적인 성능 요소이다.

3.1.2 안전성 평가항목

(1) 합의 확정 시간

블록체인에서 한 번에 두 개 이상의 노드가 블록 생성에 성공하여 체인이 분화되는 포크가 발생하거나 생성된 블록이 악의적 노드에 의해 만들어져 네트워크에 큰 문제가 생길 수 있다. 따라서 생성된 블록을 바로 체인에 등록하지 않고, 이후의 블록 생성 결과를 고려하여 블록을 확정한다. 이때 대기하게 되는 시간이 합의 확정 시간이다.

(2) Proof-of-Safety

블록체인에 참여하고자 하는 주체들 중에서 의도적으로 블록을 독점적으로 생성하거나, 체인을 왜곡하고자 하는 노드가 존재할 수 있다. Proof-of-Safety는 합의 과정에서 이와 같은 공격에 대해 감내할 수 있는 보안 성능을 의미한다.

(3) Proof-of-Liveness

악의적인 노드에 의한 공격뿐 아니라, 시스템 상의 오류나 장애 발생으로 인해 합의에 도달하는 것이 실패할 수도 있다. Proof-of-Liveness는 합의 과정에서 장애가 발생한 노드의 감내 의미한다.

3.2 분산합의 알고리즘 평가항목 분석

3.2.1 효율성 평가항목 분석

(1) 합의 노드의 수

현재까지 제안된 분산합의 알고리즘들의 경우, 합의 과정에 전체 노드가 모두 참여하는 경우와 합의 노드의 수가 특정한 상수로 정해져 있는 경우로 분류하여 분석할 수 있다.

작업 증명, 지분 증명, 중요도 증명, 소요 시간 증명 알고리즘의 경우 모든 노드가 블록의 생성에 참여하여 경쟁적으로 블록 생성 권한을 획득하고자 한다. 또한, Paxos/Raft, PBFT 알고리즘은 전체 노드가 참여하는 투표를 수행한다. 즉, 이러한 합의 알고리즘들은 블록체인에 참여하는 전체 노드의 수가 n으로 주어졌을 때, 합의 노드의 수가 n개라고 할 수 있다.

반면, 위임된 지분 증명 알고리즘 및 Tendermint알고리즘은 네트워크에 존재하는 노드의 수와는 상관없이 일정한 수의 노드만이 검증자의 역할을 수행하며 합의에 참여한다. 예를 들어, 암호화폐인 EOS는 오직 21개의 노드만이 블록 생성에 참여하고, Tendermint 알고리즘은 101개의 노드가 검증자로 참여한다.

(2) 에너지 소모량

분산합의 알고리즘의 에너지 소모량은 해시 연산과 같이 많은 연산을 요구하는 알고리즘과 그렇지 않은 알고리즘으로 분류하여 분석할 수 있다. 작업 증명 및 작업 증명과 지분 증명을 동시에 사용하는 분산합의 알고리즘에서 블록의 생성은 해시 퍼즐의 답을 찾는 해시 연산을 수행한다. 이때, 식 (1)의 난이도를 통해 해당 시점에서 평균적으로 발생할 수 있는 해시 연산의 수를 알 수 있다. 즉, 난이도를 통해 블록 생성을 위해 평균적으로 발생할 수 있는 연산량을 계산할 수 있으며, 연산 당 소모되는 전력량($W/hash\_rate$)을 토대로 블록 생성을 위한 에너지 소모량을 추정할 수 있다.

중요도 증명은 해시 함수를 사용하지만, 연산량을 토대로 이루어지는 작업 증명과는 다른 메커니즘을 사용하기 때문에, 에너지 소모량이 훨씬 더 적다. 위임된 지분 증명 알고리즘은 블록 생성 권한을 획득하기 위한 연산량 증명 과정이 제외되므로 에너지 소모량이 적다. 마찬가지로, 별도의 블록 생성 프로토콜을 가지고 있는 소요 시간 증명 알고리즘이나 블록 생성 권한이 특정 노드에게 부여된 Paxos/Raft, PBFT 및 Tendermint 합의 알고리즘 또한 반복적인 연산을 수행하지 않는다. 따라서 이러한 합의 알고리즘을 통해 블록을 생성할 때에는 작업 증명과 같은 분산합의 알고리즘과는 다르게 연산량에 의한 별도의 에너지 소모가 발생하지 않는다. 즉, 블록을 생성할 때 에너지 소모량이 시스템을 운용하기 위한 최소한의 에너지 소모량과 같으며, 상대적으로 매우 적은 수준이다.

(3) 초당 트랜잭션 처리량(Transaction Per Second, TPS)

분산합의 알고리즘의 초당 트랜잭션 처리량은 다음과 같이 분석할 수 있다. 만약, 블록의 생성 시간을 t, 블록의 크기를 S_b, 트랜잭션의 크기를 S_t라고 할 때, 초당 트랜잭션 처리량은 식 (4)와 같이 계산할 수 있다.

$$TPS = \frac{S_b}{S_t} \cdot \frac{1}{t} \tag{4}$$

예를 들어, 작업 증명 알고리즘을 이용하는 비트코인은 600초당 하나의 블록을 생성하고, 블록과 트랜잭션의 크기가 각각 1MB, 250byte이기 때문에 위 식에 대입하면 초당 약 7개의 트랜잭션을 처리할 수 있다.

해당 모델은 모든 분산합의 알고리즘에 적용 가능하지만 보다 구체적인 초당 트랜잭션 처리량의 계산은 분산합의 알고리즘의 종류 뿐 아니라, 응용되는 블록체인의 설정에 따라 달라지는 측면이 있다. 예를 들어, 같은 작업 증명 알고리즘을 사용하지만 이더리움은 블록 사이즈의 제한이 없어 이론상으로 매우 많은 트랜잭션을 처리할 수 있으나, 운영의 안전성 측면에서 비트코인보다 많은 15개의 초당 트랜잭션만을 처리하고 있다.

<Table 1>은 세 가지 효율성 평가항목에 대한 분산합의 알고리즘의 분석 결과를 정리한 것이다.

<Table 1> Summary of Efficiency Analysis

	# of consensus nodes	Energy consumption	TPS
PoW	n	Depends on difficulty of hash puzzle	$\frac{S_b}{S_t} \cdot \frac{1}{t}$
PoS	n	Depends on difficulty of hash puzzle	
DPoS	$c(<n)$	Very small	
PoI	n	Very small	
PoET	n	Very small	
Paxos/Raft	n	Very small	
PBFT	n	Very small	
Tendermint	$c(<n)$	Very small	

3.2.2 안전성 평가항목 분석

(1) 합의 확정 시간

합의 확정 시간은 포크가 발생할 수 있어 합의 확정 블록을 필요로 하는 알고리즘에서 고려가 필요하다. 이에 대해 Satoshi[14]는 비트코인을 제안하는 논문에서 악의적인 노드가 블록 생성을 통해 체인을 성공적으로 공격할 확률 P를 식 (5)와 같이 정의하였다[3].

$$P=1-\sum_{k=0}^{z}\frac{\lambda^k e^{-\lambda}}{k!}(1-(q/p)^{(z-k)}) \quad (5)$$

이때, p는 정직한 노드가 블록을 생성할 확률, q는 공격자가 블록을 생성할 확률이며$(p+q=1)$, z는 확정까지 기다려야 하는 블록의 수를 의미한다. 즉, 더 많은 블록을 대기할수록 공격의 성공률은 더욱 낮아짐을 알 수 있다. 최종적으로는 블록 생성 시간과 대기해야 하는 블록의 수 z의 곱으로 합의 확정 시간을 계산할 수 있다. 대표적으로, 비트코인의 경우 $z=6$의 값을 이용하며, 블록 생성 시간은 10분이기 때문에 합의 확정 시간은 60분(1시간)이다. 이와 같은 합의 확정 시간 모델은 작업 증명 알고리즘을 제안하는 논문에서 최초로 기술되었으나, 포크가 발생할 수 있는 모든 분산합의 알고리즘(작업 증명, 지분 증명, 위임된 지분 증명, 중요도 증명)에서 공통적으로 사용될 수 있다.

반면, 소요 시간 증명 알고리즘은 블록을 검증하기 위한 통계적 검증 과정이 프로토콜에 정의되어 있기 때문에 별도의 블록 확정 시간을 필요로 하지 않는다. Paxos/Raft, PBFT 및 Tendermint 합의 알고리즘 또한 투표에 따라 블록을 검증하고 바로 확정하기 때문에 합의 확정을 위한 별도의 시간이 필요하지 않다.

(2) Proof-of-Safety

분산합의 알고리즘의 Proof-of-Safety는 합의 확정 시간 모델을 사용할 수 있는 경우와 그렇지 않은 경우로 분류하여 분석할 수 있다.

합의 확정 시간 모델을 사용할 수 있는 분산합의 알고리즘의 경우, 식 (5)를 이용하여 Proof-of-Safety를 계산할 수 있다. 만약, 식 (5)에서 악의적인 노드가 블록을 생성할 확률 q가 1/2보다 크다면$(q \geq 1/2, p \leq 1/2)$, 공격이 성공할 확률 P는 1이 된다. 이때, 악의적인 노드가 블록을 생성할 확률 q는 각각의 분산합의 알고리즘에서 악의적인 노드가 차지하고 있는 자원의 비중이라고 할 수 있다. 예를 들어, 해시 연산을 통해 블록을 생성하는 작업 증명 알고리즘에서 자원을 생성할 확률은 해시 연산을 수행할 수 있는 능력에 비례한다. 즉, 네트워크가 가진 전체 해시 연산 능력의 50% 이상을 악의적인 노드가 차지한다면 합의 확정 시간에 상관없이 공격이 무조건 성공한다. 마찬가지로, 지분 증명 알고리즘에서 악의적인 노드가 전체 지분의 50% 이상을 점유하였을 때에도 공격을 막을 수 없다. 결과적으로, 이와 같은 분산합의 알고리즘에서 Proof-of-Safety는 50%라고 할 수 있다.

소요 시간 증명 알고리즘은 블록을 검증하는 프로토콜이 존재하지만 복수의 노드가 담합의 형태로 블록을 독과점하는 형태의 공격이 가능하다. 이때, 성공적으로 독과점을 수행하기 위해 담합해야 하는 노드의 비율 ϕ는 전체 노드의 수 n에 대해 식 (6)과 같이 계산된다[9]. 즉, 소요 시간 증명 알고리즘은 전체 노드 수 n에 비례하여 Proof-of-Safety가 결정되는 분산합의 알고리즘이다.

$$\phi=\theta\left(\frac{\log\log n}{\log n}\right) \quad (6)$$

PBFT 알고리즘은 전체 노드의 수 n을 결정할 때, 허용 가능한 악의적인 노드의 수 f를 고려하여 결정한다. 구체적으로는 $n=3f+1$이 되도록 블록체인 네트워크를 설계하며, 이에 따라 Proof-of-Safety는 1/3 = 33%가 된다. 다시 말해, 전체 노드 중 공격자 노드의 비율이 1/3 미만이라면 합의 도출에 문제가 없다. PBFT 알고리즘의 합의 프로토콜을 공유하는 Tendermint 합의 알고리즘 역시 마찬가지로 33%의 Proof-of-Safety를 갖는다. 그러나 PBFT의 33% Proof-of-Safety가 전체 노드의 33%를 의미하는 반면, Tendermint 합의 알고리즘에서는 합의 과정에서 지분에 비례하여 주어지는 투표권의 33%를 의미한다는 차이가 있다. 그 외에도, Paxos/Raft 알고리즘은 비잔틴 노드를 고려하지 않기 때문에 Proof-of-Safety가 존재하지 않는다.

(3) Proof-of-Liveness

현재 사용되는 대부분의 분산합의 알고리즘들의 경우, Proof-of-Safety와 Proof-of-Liveness가 동일한 값을 가진다[13]. 그러나 예외적으로, Paxos/Raft 알고리즘은 전체 노드의 수 n을 결정할 때, 허용 가능한 장애 발생 노드의 수 f'를 고려하여 결정한다. 구체적으로는 $n=2f'+1$이 되도록 블록체인 네트워크를 설계하기 때문에, 50%의 Proof-of-Liveness를 가진다.

<Table 2>는 세 가지 안정성 평가항목에 대한 분산합의 알고리즘의 분석 결과를 정리한 것이다.

<Table 2> Summary of Safety Analysis

	Consensus confirmation time	Proof-of-safety	Proof-of-Liveness
PoW	$z \cdot t$	50%	50%
PoS	$z \cdot t$	50%	50%
DPoS	$z \cdot t$	50%	50%
PoI	$z \cdot t$	50%	50%
PoET	No Confirmation	$\theta\left(\frac{\log \log n}{\log n}\right)$	$\theta\left(\frac{\log \log n}{\log n}\right)$
Paxos/Raft	No Confirmation	N/A	50%
PBFT	No Confirmation	33%	33%
Tendermint	No Confirmation	33%	33%

4. 새로운 평가항목 및 성능 개선 방안

4.1 필요성

분산합의 알고리즘은 분산합의 주체를 선정하는 과정에서 새로운 블록 생성에 대한 권한을 갖게 된 노드가 정당하게 해싱 결과를 생성하였는지 모든 참여 노드가 확인할 수 있도록 하는 방법을 제시하는 것이 필요하다. 그러나 이를 위해 각 노드가 발생시킨 난스 값을 모든 노드에게 공개한다면, 그것을 기반으로 블록 생성에 참여할 노드를 미리 계산할 수 있게 되어 노드 간 담합에 의한 공격이 가능해지는 문제가 발생할 수 있으며, 악의적인 노드가 특정 노드의 난스 값을 사용할 수 있는 문제가 발생할 수 있다. 따라서 이러한 문제를 해결하기 위해서는 노드가 사용한 난스 값이 그 노드의 것임을 다른 노드들이 확인할 수 있어야 하며, 동시에 새로운 블록 생성에 참여하는 노드들을 다른 노드들이 미리 예측할 수 없도록 해야 한다.

또한 기존 분산합의 알고리즘에서는 분산합의 주체가 전체 또는 일부분으로 미리 고정되어 있다. 그러나 지나치게 많은 노드가 분산합의 주체로 선정된다면, 네트워크 트래픽이 증가하고 합의를 위해 긴 시간이 소모될 수 있다. 반면, 분산합의 주체가 너무 적다면, 합의에 필요한 최소 노드 이하가 선정되어 합의가 불가능해 질 수도 있다. 따라서 분산합의에 필요한 주체 개수를 제어할 수 있는 적합한 방법이 필요하며, 이를 통해 블록체인의 단점 중 하나인 합의에 필요한 시간을 줄이고, 네트워크 효율성을 높일 수 있는 방안이 필요하다.

제 4장에서는 이와 같이 기존 분산합의 알고리즘의 성능 개선을 위해서 필요한 합의 주체 불예측성과 블록 생성 권한 확인을 위한 방안을 제시한다. 또한 분산합의에 필요한 최소한의 노드만 자격을 얻을 수 있도록 하기 위한 분산합의 주체 수 제어 방안을 제안하고자 한다. 이를 위해, 블록체인에서 식 (7)을 사용하여 height h를 갖는 블록이 확률 p로 생성되는 경우를 고려한다.

$$hash(header_{hash_{h-1}}), nonce_h) < difficulty_h \qquad (7)$$

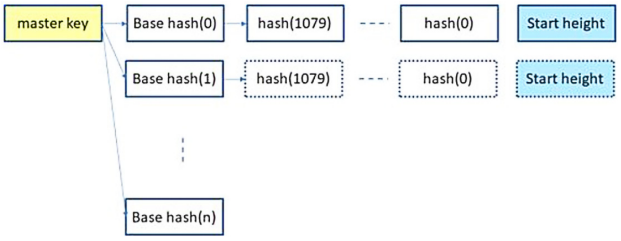
여기서 $header_{hash_{h-1}}$과 $nonce_h$는 height $h-1$ 블록의 헤더 해시 값과 height h에 대해 노드가 발생시킨 난스 값을 나타낸다.

4.2 합의 주체 불예측성 및 블록 생성 권한 확인 방안

먼저 블록체인의 합의 주체 불예측성 보장을 위한 방안으로 본 논문에서는 난스 체인을 사용하는 방법을 제안한다. 먼저, 각 노드는 마스터 키와 하나의 임의의 수(count)를 정한 후, 이들을 해싱하여 base hash를 생성한다. 그 후, 이 값을 씨드(seed) 값으로 해싱하여 다음 해시 값을 계산하고, 계산된 해시 값을 다시 해싱하여 다음 해시를 계산하는 방법으로 연결된 하나의 난스 체인을 만든다. 정해진 길이의 난스 체인을 하나 생성한 수, 임의의 수(count)를 1씩 증가시키면서 마스터 키를 이용한 해싱을 통해 새로운 base hash 값을 이용한 난스 체인을 계속 생성할 수 있다. <Figure 5>는 이런 방법을 적용하여 생성된 $n+1$개의 bash hash로 구성된 난스 체인의 예를 나타낸다. 이때, 각 난스 체인의 길이는 1,080으로 가정되었으며, 이는 블록을 10초에 한 번 생성할 경우 3시간 동안 사용할 수 있는 난스의 개수(6×60×3 = 1,080)이다.

블록 생성에 참여하고자 하는 노드는 이렇게 생성된 난스 체인의 마지막 해시 값 hash(0)와 이 해시 값의 사용이 시작될 블록의 height만을 모든 노드들에게 공개한다. 그 이후로는 "생성될 블록의 height h-start height"에 해당하는 해시 값 $nonce_h$를 난스 체인에서 가져와 이전 블록의 해시 값과 같이 해싱하여 난수를 계산한 후, 식 (7)을 이용하여 블록 생성 참여 여부를 결정한다. 이 때, 해당 노드는 난스 체인에서 가져온 난스 값 $nonce_h$를 모든 노드에게 공개한다.

이러한 과정에서 해당 노드가 정당하게 블록 생성에 참여하였음을 증명하기 위해서 다른 노드들은 블록 생성 참여 노드가 공개한 해시 값 $nonce_h$를 "생성될 블록의 height h-start height"번 해시 연산을 반복하고, 그 값이 블록 생성 참여 노드가 미리 공개한 hash(0) 값과 같은지를 확인할 수 있다.



<Figure 5> Example of Nonce Chain

따라서 자신을 제외한 모든 노드는 서로 난스 체인의 해시 값을 예측할 수 없으므로 노드들 간 담합에 의해 미리 블록 생성에 참여 가능한 노드를 예측하는 것이 불가능하게 된다. 또한, 노드가 계산에 의해 블록 생성에 참여가 결정되는 경우, 해당 난스 체인 값을 공개하여 정당한 해시 값을 가졌는지 증명할 수 있게 된다.

4.3 분산합의 주체 수 제어 방안

만일 분산합의 주체를 결정하기 위해 식 (7)과 같은 방법을 이용한다면, n개의 노드들이 각각 임의의 랜덤 값을 하나씩 생성하고, 각 노드가 계산한 값을 임계치 difficulty와 비교하여 조건을 만족하는 경우에만 합의 주체가 될 수 있다. 따라서 각각의 노드들에 대한 이 테스트는 분산합의 주체 선정(성공) 확률이 p인 베르누이 시행이 된다.

만일 전체 노드 수가 n이고, 선정될 분산합의 주체 개수를 X라고 하면, X는 평균과 분산이 각각 $\mu = np$, $\sigma^2 = np(1-p)$인 이항분포를 하며, n이 충분히 큰 경우 중심극한 정리에 의해 정규분포 $N(np, np(1-p))$로 수렴한다. 이때, X의 누적분포함수 $F(x)$는 식 (8)과 같이 표현될 수 있다.

$$F(x) = \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{(y-\mu)^2}{2\sigma^2}} dy \tag{8}$$

$$= \frac{1}{2}\left(1 + erf\left(\frac{x-\mu}{\sigma\sqrt{2}}\right)\right)$$

만일 노드가 x개 이하로 선택될 확률을 $F(x) = k$라고 하면,

$$k = \frac{1}{2}\left(1 + erf\left(\frac{x-\mu}{\sigma\sqrt{2}}\right)\right) \tag{9}$$

이고, 이는 식 (10)과 같이 μ에 대한 2차 방정식으로 표현될 수 있다.

$$\left(\frac{2a}{n}+1\right)\mu^2 - 2(x+a)\mu + x^2 = 0 \tag{10}$$

이때, $a = (erf^{-1}(2k-1))^2$이며, 식 (10)의 해는 식 (11)과 같이 구할 수 있다.

$$\mu = \frac{x+a+\sqrt{(x+a)^2 - \left(\frac{2a}{n}+1\right)x^2}}{\left(\frac{2a}{n}+1\right)} \tag{11}$$

따라서 x와 k가 주어진 경우, 각 노드가 합의 주체로 선택될 확률은 $\mu = np$에 의해 식 (12)와 같이 정해질 수 있다. 이때, k는 정해진 기간 동안 생성된 블록 중 1개가 분산합의 주체가 x개 이하일 때 생성된 경우의 확률을 나타낸다. 즉, 10초에 한번 블록을 생성하는 경우, 1년 동안 발생하는 누적 블록 수는 6×60×24×365 = 3,153,600개이므로 $k = \frac{1}{3,153,600}$이라고 하면, 이 값은 분산합의 주체로 x개 이하의 노드가 선정될 확률을 의미하며, 이러한 경우가 1년에 1번 발생한다는 의미를 갖는다.

$$p_{x,k} = \frac{x+a+\sqrt{(x+a)^2 - \left(\frac{2a}{n}+1\right)x^2}}{2a+n} \tag{12}$$

식 (7)에서 모든 노드가 사용할 임계치 difficulty는 계산된 해시 값의 일부분이 표현할 수 있는 최대값 $\max_{slice}$(예를 들어 32비트를 사용하는 경우 $\max_{slice} = 2^{32}$)에 $p_{x,k}$를 곱하여 식 (13)과 같이 정할 수 있다. 이것은 확률 $p_{x,k}$를 사용할 때, 표현 가능한 수의 평균을 difficulty로 사용한다는 의미이다.

$$difficulty = p_{x,k} \times \max_{slice} \tag{13}$$

5. 결 론

본 논문에서는 블록체인에서 사용되는 기존 분산합의 알고리즘의 성능을 평가할 수 있는 항목을 효율성과 안전성 지표로 나누어 제시하고, 지금까지 제안된 분산합의 알고리즘의 성능을 분석하였다. 또한, 기존 분산합의 알고리즘의 성능을 개선하기 위한 평가항목으로 분산합의 주체의 불예측성, 블록 생성 권한 확인 및 분산합의 주체 수 제어 등을 제안하였으며, 이를 구현하기 위한

방안으로 난스 체인을 이용하는 방법과 분산합의 주체 수를 제어하기 위한 베르누이 시행 기반 선정 확률을 이용하는 방안에 대해서 제안하였다.

이러한 연구 결과를 바탕으로 향후 난스 증명을 기반으로 한 새로운 분산합의 알고리즘을 설계하고자 하며, 블록체인을 위한 활용을 검증할 수 있는 플랫폼을 개발하고자 한다. 이러한 새로운 분산합의 알고리즘은 기존의 PoW 또는 PoS 등이 가지고 있는 한계점을 개선할 수 있으며, 그 결과로 좀 더 다양한 응용 분야로 확대될 수 있을 것으로 기대된다.

Acknowledgements

This work was supported by Electronics and Telecommunications Research Institute (ETRI) grant funded by the Korean government [No. 2018-0-0020, Development of High Confidence Information Trading Platform Based on block chain (PON algorithm)].

References

[1] Azaria, A., Ekblaw, A., Vieira, T., and Lippman, A., Medrec : Using blockchain for medical data access and permission management, *In conference on Open and Big Data (OBD)*, Vienna, Austria, 2016, pp. 25-30.

[2] Baliga, A., Understanding blockchain consensus models, *Persistent*, 2017, pp. 1-14.

[3] Bitcoin Energy Consumption Index, https://digiconomist.net/bitcoin-energy-consumption.

[4] BitFury Group, Proof of Stake versus Proof of Work, http://bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf.

[5] Buchman, E., Tendermint : Byzantine fault tolerance in the age of blockchains [dissertation], [Guelph, Canada] : University of Guelph, 2016.

[6] Buterin, V., What proof of stake is and why it matters, *Bitcoin Magazine*, 2013, pp. 1-3.

[7] Castro, M. and Liskov, B., Practical Byzantine fault tolerance, *OSDI*, 1999, Vol. 99, pp. 173-186.

[8] Chandra, T.D., Griesemer, R., and Redstone, J., Paxos made live : an engineering perspective, *In Proceedings of the twenty-sixth annual ACM symposium on Principles of distributed computing*, Portland, USA, 2007, pp. 398-407.

[9] Chen, L., Xu, L., Shah, N., Gao, Z., Lu, Y., and Shi, W., On security analysis of proof-of-elapsed-time(PoET), *In International Symposium on Stabilization, Safety, and Security of Distributed Systems*, Boston, USA, 2017, pp. 282-297.

[10] Haber, S. and Stornetta, W. S., How to time-stamp a digital document, *In Conference on the Theory and Application of Cryptography*, Berlin, Germany, 1990, pp. 437-455.

[11] King, S. and Nadal, S., Ppcoin : Peer-to-peer crypto-currency with proof-of-stake, https://peercoin.net/assets/paper/peercoin-paper.pdf.

[12] Miller, D., Blockchain and the Internet of Things in the Industrial Sector, *IT Professional,* 2018, Vol. 20, No. 3, pp. 15-18.

[13] Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W., and Qijun, C., A review on consensus algorithm of blockchain, *In Conference on Systems, Man, and Cybernetics (SMC)*, Banff, Canada, 2017, pp. 2567-2572.

[14] Nakamoto, S., Bitcoin : A peer-to-peer electronic cash system, https://bitcoin.org/bitcoin.pdf.

[15] Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S., Bitcoin and cryptocurrency technologies : a comprehensive introduction, Princeton University Press, 2016, pp. 52-57.

[16] NEM group, NEM Technical Reference, https://www.cryptoground.com/storage/files/1527489057_NEM_techRef.pdf.

[17] Pilkington, M., Research handbook on digital transformations, Edward Elgar Publishing, 2016, pp. 225-253.

[18] Tapscott, A. and Tapscott, D., How blockchain is changing finance, *Harvard Business School Publishing*, 2017, pp. 1-5.

[19] The Raft Consensus Algorithm, http://raft.github.io.

[20] Tian, F., An agri-food supply chain traceability system for China based on RFID & blockchain technology, *In Conference on Service Systems and Service Management (ICSSSM)*, Kunming, China, 2016, pp. 1-6.

[21] World Economic Forum, The global competitiveness report, http://www3.weforum.org/docs/GCR2016-2017/05FullReport/TheGlobalCompetitive nessReport2016-2017_FINAL.pdf.

ORCID

Do Gyun Kim | http://orcid.org/0000-0002-5149-9417
Jin Young Choi | http://orcid.org/0000-0001-6397-3107
Ki Young Kim | http://orcid.org/0000-0001-5059-2284
Jintae Oh | http://orcid.org/0000-0002-4372-0943